

Serial No. 09/763,271

IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered). Please AMEND claims 1, 2, 3, 5, 11, 21 and 23 in accordance with the following:

1. (currently amended): A method for producing a regenerated private key by a computer for a predetermined asymmetric cryptographic key pair which includes an original private key and a corresponding public key, the regenerated private key being identical to the original private key, the original private key and the public key having been generated by receiving a predetermined initial value entered by a user; processing the predetermined initial value to obtain a base value for obtaining first and second prime numbers; checking whether the base value is a prime number and, when the base value is not a prime number, increasing the base value by a predetermined increment to obtain a new value; repeating the step of checking until the first and second prime numbers are obtained; storing an index to obtain a stored index, the stored index being a number indicating how oftenmany times, in the step of checking, the base value has been increased until the first prime number or the second prime number are obtained; calculating the original private key using the first and second prime numbers; and calculating the public key using the original private key and the first and second prime numbers, the method comprising:

receiving a user input of the predetermined initial value by the computer;
processing the predetermined initial value to obtain a base value for obtaining the first and second prime numbers;

increasing the base value by a value determined by the index previously stored and the predetermined increment to obtain the first and second prime numbers; and
calculating the regenerated private key using the first and second prime numbers.

2. (currently amended): The method according to claim 1,
wherein, wherein the process of obtaining the original private key, the predetermined initial value is supplied to a hash function to obtain the base value; and
wherein, wherein the process of obtaining the regenerated private key, the same hash

Serial No. 09/763,271

function is used.

3. (currently amended): The method according to claim 1,
wherein, wherein the process of obtaining the original private key, the predetermined
initial value is supplied to a hash function to obtain the base value, and
wherein, wherein the process of obtaining the regenerated private key, the same hash
function is used in the step of processing the, and
the respective values formed by the hash function are used in the determination of both
an original key pair and a regenerated key pair.

4. (cancelled).

5. (currently amended): The method according to claim 1, wherein, wherein the
process of generating the original private key and the public key,-of the method of Miller-
Rabin is used when checking to check whether the base value is a prime number.

6. (previously presented): The method according to claim 1,
wherein the asymmetric cryptographic key pair is formed according to the RSA
method.

7. (previously presented): The method according to claim 2, wherein the hash
function is one of the following methods:

- MD-5 method,
- the MD-2 method, and
- method according to the data encryption standard (DES) as a one-way function.

8. (previously presented): The method according to claim 1, further comprising the
following :

using the regenerated private key for encryption electronic data.

9. (previously presented): The method according to claim 1, further comprising :
using the regenerated private key for forming a digital signature.

10. (previously presented): The method according to claim 1, further comprising the

Serial No. 09/763,271

following step:

using the regenerated private key for an authentication.

11. (currently amended): A system to form a regenerated private key for a predetermined asymmetric cryptographic key pair, which includes an original private key and a corresponding public key, the regenerated private key being identical to the original private key, the original private key and the public key having been generated by receiving a predetermined initial value entered by a user; processing the predetermined initial value to obtain a base value for obtaining first and second prime numbers; checking whether the base value is a prime number and, when the base value is not a prime number, increasing the base value by a predetermined increment to obtain a new value; repeating the step of checking until the first and second prime numbers are obtained; storing an index to obtain a stored index, the stored index being a number indicating how oftenmany times, in the step of checking, the base value has been increased until the first prime number or the second prime number are obtained; calculating the original private key using the first and second prime numbers; and calculating the public key using the original private key and the first and second prime numbers, the system comprising:

an input device to receive a user input of the predetermined initial value;

a processor to process the predetermined initial value to obtain the base value for obtaining the first and second prime numbers, to increase the base value by a value determined by the stored index and the predetermined increment to obtain the first prime number or the second prime number; and to produce the regenerated private key using the first prime number and the second prime number.

Claims 12-20 (Cancelled)

21. (currently amended): A method for generating an asymmetric cryptographic key pair having a public key and a private key, comprising:

receiving a predetermined initial value entered by a user;

processing the predetermined initial value to obtain a base value for obtaining first and second prime numbers;

checking whether the base value is a prime number and, when the base value is not a prime number, increasing the base value by a predetermined increment to obtain a new value;

repeating the step of checking, until the first and second prime numbers are obtained,

Serial No. 09/763,271

storing an index indicating how oftenmany times, in the step of checking, the base value has been increased until the first prime number or the second prime number is obtained;
calculating the private key using the first prime number and the second prime number;
calculating the public key using the private key, the first prime number and the second prime number, and
erasing the private key.

22. (previously presented): A method in accordance with claim 21, wherein the private key is used in a cryptographic operation, and erasing is performed after using the private key in the cryptographic operation.

23. (currently amended): An apparatus for generating an asymmetric cryptographic key pair having a public key and a private key, comprising:

means for receiving a predetermined initial value entered by a user;
means for processing the predetermined initial value to obtain a base value for obtaining first and second prime numbers;
means for checking, whether the base value is a prime number and, when the base value is not a prime number, increasing the base value by a predetermined increment to obtain a new value;
means for repeating the step of checking, until the first and second prime numbers are obtained,
means for storing an index indicating how oftenmany times, in the step of checking, the base value has been increased until the first prime number or the second prime number is obtained;
means for calculating the private key using the first prime number and the second prime number;
means for calculating the public key using the private key, the first prime number and the second prime number; and
means for erasing the private key.